

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. – 29. (Cancelled)

30. (Previously Presented) An apparatus arranged for receiving an access request in a telecommunication core network (CN) from an entity (WLAN-AS) in an access network (WLAN) where a user with a user's equipment (UE) accesses through, the user being a subscriber of the telecommunication CN and being identified by a user's identifier included in the access request, the apparatus having a means for carrying out an authentication procedure with the UE through the access network (WLAN) in order to authenticate the user; and a means for computing at least one secret user's key (Kc) usable as cryptographic material, the apparatus comprising:

a means for deriving from the cryptographic material a user's shared key (SSO\_key-1) intended for SSO purposes; and

a means for sending the user's shared key (SSO key-1) along with the user's identifier towards a session manager (SSO\_SM) serving a service network (SN).

31. (Previously Presented) The apparatus of claim 30, further comprising means for being notified that a session at the access level has been established, this notification triggering the sending of the user's shared key (SSO\_key-1) towards the session manager (SSO\_SM) serving the service network (SN).

32. (Previously Presented) The apparatus of claim 31, further comprising means for being notified that a session at the access level has been terminated, and means for forwarding this notification towards the session manager (SSO\_SM) serving the service network (SN) in order to inactivate a current master session for the user.

33.-45. (Canceled)

46. (Previously Presented) A user's equipment (UE) usable by a user with a subscription in a telecommunication network, and arranged to access a telecommunication service network (SN) through an access network (WLAN), the user's equipment (UE) having means for carrying out an authentication procedure to authenticate the user with a core network (CN), where the user holds the subscription, through the access network (WLAN) and means for computing at least one secret user's key (Kc) usable as cryptographic material, the user's equipment comprising:

a means for deriving from the cryptographic material a user's shared key (SSO\_key-2) intended for SSO purposes;

a repository for storing the user's shared key (SSO\_key-2); and

a means for confirming the user's shared key (SSO\_key-2) stored at the user's equipment towards an entity (SAAN, SSO\_SM) in the service network (SN).

47. (Previously Presented) The user's equipment of claim 46, wherein the means for confirming includes a means for downloading an SSO plug-in from an entity (SAAN, SSO\_SM) in the service network (SN), the SSO plug-in running for confirming back the user's shared key.

48. (Previously Presented) The user's equipment of claim 46, wherein the means for confirming includes a means for processing the user's shared key (SSO\_key-2) to obtain a key code (MAC(SSO\_key-2)) to be transmitted to an entity (SAAN, SSO\_SM) in the service network (SN).

49. (Previously Presented) The user's equipment of claim 46, further comprising means for receiving an SSO cookie from an entity (SAAN, SSO\_SM) in the service network, the SSO cookie to be included in all further service requests from the user's equipment as an SSO token.

50.-58 (Cancelled)